Amazon Web Services: Visão geral do processo de segurança

Maio de 2011

(Consulte o http://aws.amazon.com/security **para obter a versão mais recente deste documento)**

A Amazon Web Services (AWS) fornece uma plataforma de computação em nuvem escalável com alta confiabilidade e disponibilidade, oferecendo a flexibilidade que permite aos clientes a criação de uma ampla variedade de aplicativos. Ajudar a proteger a confidencialidade, a integridade e a disponibilidade de sistemas e dados de nossos clientes é de suma importância para a AWS, da mesma forma que é importante também manter a confiança dos clientes. Este documento destina-se a responder várias perguntas, dentre elas: "Como a AWS pode me ajudar a proteger meus dados?" Especificamente, os processos de segurança física e operacional da AWS são descritos para fins de infraestrutura de rede e de servidores sob a gestão da AWS, bem como implementações de segurança específicas do serviço. Este documento fornece uma visão geral de segurança no que se refere às seguintes áreas relevantes para a AWS:

- Ambiente de responsabilidade compartilhada
- Resumo do ambiente de controle
- Princípios de Design seguro
- Backup
- Monitoramento
- Informações e comunicação
- Ciclo de vida do funcionário
- Segurança física
- Proteções ambientais
- Gerenciamento de configuração
- Gerenciamento de continuidade de negócios
- Backups
- Separação de falhas
- Recursos de segurança da conta da Amazon
- Segurança de rede
- Segurança específicas do serviço AWS
    - Segurança do Amazon Elastic Compute Cloud (Amazon EC2)
    - Amazon Virtual Private Cloud (Amazon VPC)
    - Segurança do Amazon Simple Storage Service (Amazon S3)
    - Segurança do Amazon SimpleDB
    - Segurança do Amazon Relational Database Service (Amazon RDS)
    - Segurança do Amazon Simple Queue Service (Amazon SQS) Security
    - Segurança do Amazon Simple Notification Service (SNS) Security
    - Segurança do Amazon CloudWatch Security
    - Segurança do Auto Scaling Security
    - Segurança do Amazon CloudFront Security
    - Segurança do Amazon Elastic MapReduce Security

Ambiente de responsabilidade compartilhada

Ao mover a infraestrutura de TI para a AWS cria-se um modelo de responsabilidade compartilhada entre o cliente e a AWS. Este modelo compartilhado pode auxiliar a diminuir as preocupações operacionais do cliente em relação aos componentes do sistema operacional do host no qual a AWS opera, administra e controla e para o controle da camada de virtualização em baixa para a segurança física das instalações em que o serviço opera. O cliente assume a gestão e a responsabilidade pelo sistema operacional convidado (inclusive atualizações e patches de segurança), por outro software de aplicativo associado, bem como pela configuração do grupo de segurança firewall fornecido pela AWS. Os clientes devem examinar cuidadosamente os serviços que escolherem, assim como as suas respectivas responsabilidades que variam de acordo com os serviços utilizados, a integração desses serviços no seu ambiente de TI e as leis e regulamentos aplicáveis. Isto é possível para os clientes com o propósito de aumentar a segurança e/ou atender aos seus mais rigorosos requisitos de conformidade, aproveitando tecnologias tais como firewalls baseados em host, detecção/prevenção de invasões, criptografia e gerenciamento de chaves, baseados em host. A natureza desta responsabilidade compartilhada também fornece a flexibilidade e o controle do cliente que permite a implantação de soluções que atendam aos requisitos de certificação específicos do setor.

Resumo do ambiente de controle

A AWS gerencia um ambiente de controle abrangente que inclui as atividades políticas, os processos e o controle necessários para a disponibilização de cada uma das ofertas de serviços web. O ambiente de controle coletivo abrange as pessoas, os processos e a tecnologia necessários para manter um ambiente que ofereça suporte a eficácia de controles específicos e dos quadros de controle para o qual a AWS possui certificação e/ou está em conformidade.

A AWS está em conformidade com várias certificações e atestados de terceiros. Dentre eles estão:

- **SAS70 Tipo II.** Este relatório inclui controles detalhados que a AWS executa junto com um parecer de auditor independente sobre a eficácia do funcionamento desses controles.
- **PCI DSS Nível 1.** A AWS foi validada independentemente para estar em conformidade com o padrão de segurança de dados PCI como um provedor de serviços de host compartilhado.
- **ISO 27001.** A AWS obteve a certificação ISO 27001 do nosso sistema de gestão de segurança da informação (ISMS - Information Security Management System) que abrange a infraestrutura, datacenters e serviços
- **FISMA.** A AWS permite que os clientes da Agência de governo alcancem e mantenham a conformidade com a Gestão de segurança de informação Federal (FISMA). A AWS foi certificada e acreditada para operar em nível FISMA baixo. E concluiu também a implementação de controle e passou com sucesso nos testes e na avaliação de segurança independentes necessários para operar a nível FISMA-moderado. A AWS atualmente busca obter uma aprovação das agências governamentais para operar a nível FISMA moderado.

Além disso, os clientes criaram aplicativos na área de saúde em conformidade com as Regras de privacidade e segurança do **HIPPA** na AWS**.**

Mais informações sobre essas certificações e atestados de terceiros estão disponíveis no Whitepaper de risco e conformidade disponível no site: http://aws.amazon.com/security.

Princípios de Design seguro

O processo de desenvolvimento da AWS segue as melhores práticas de desenvolvimento de software seguro, que incluem revisões de design formal pelo AWS Security Team, a modelagem de ameaças e a conclusão de uma avaliação de risco. Ferramentas de análise de código estático são executadas como parte do processo de compilação padrão, e todo o software implantado é submetido a testes de penetração recorrentes realizados por especialistas do setor

cuidadosamente selecionados. Nossas revisões de avaliação de riscos de segurança se iniciam durante a fase de design e o engajamento dura o tempo do lançamento até as operações em curso.

Monitoramento

A AWS utiliza sistemas de monitoramento automatizados para fornecer um alto nível de disponibilidade e desempenho do serviço. O monitoramento proativo está disponível através de uma variedade de ferramentas on-line para uso interno e externo. Sistemas dentro da AWS são extensivamente instrumentados para monitorar métricas operacionais chave. Os alarmes são configurados para notificar operações e gerenciar colaboradores quando limites de alerta de início são cruzados nas principais métricas operacionais. Uma agenda de plantão é usada para que colaboradores estejam sempre disponíveis para auxiliar com problemas operacionais. Isso inclui um sistema de pager para que os alertas sejam comunicados rápida e confiavelmente à equipe de operações.

A documentação é mantida para ajudar e para informar os colaboradores do setor de operações quando do tratamento de incidentes ou problemas. Se a solução de um problema exige colaboração, um sistema de conferência que oferece suporte aos recursos de comunicação e de registro será utilizado. Líderes treinados de chamada facilitam a comunicação e o progresso durante o tratamento de problemas operacionais que requerem colaboração. Post-mortems são convocadas após qualquer problema operacional significativo, independentemente do impacto externo, e documentos de causa de erro (COE) são elaborados para que a causa raiz seja descoberta e ações preventivas sejam tomadas no futuro. A implementação de medidas preventivas é controlada durante reuniões semanais de operações.

Informações e comunicação

A AWS implementou diversos métodos de comunicação interna a nível mundial para ajudar os funcionários a compreenderem suas responsabilidades e funções individuais e a comunicarem eventos significativos em tempo hábil. Esses métodos incluem orientação e programas de treinamento para funcionários recém-contratados; reuniões regulares de gerenciamento para atualizações sobre desempenho dos negócios e outros assuntos; meios eletrônicos, tais como videoconferência, mensagens de correio eletrônico e postagem de informações através da intranet da Amazon.

A AWS também implementou diversos métodos de comunicação externa para dar suporte a sua base de clientes e à comunidade. Há mecanismos em vigor para permitir que o cliente ofereça suporte a equipe para ser notificado sobre problemas operacionais que afetam a experiência do cliente. Um "Console de status de serviço" está disponível e é mantido pela equipe de suporte para alertar os clientes sobre quaisquer problemas que possam ser de grande impacto. Um “de Segurança e Conformidade” também está disponível para fornecer aos clientes um local único onde encontrar detalhes de segurança e conformidade da AWS.

Os clientes podem se inscrever para ofertas de suporte Premium que incluem uma comunicação direta com a equipe de suporte ao cliente e alertas proativos para quaisquer problemas de impacto dos clientes.

Ciclo de vida do funcionário

A AWS estabeleceu procedimentos e políticas formais para delinear as normas mínimas de acesso lógico aos hosts da plataforma e da infraestrutura AWS. A AWS exige que funcionários com necessidade de acesso aos dados dos clientes passem por uma detalhada verificação de antecedentes (conforme o permitido por lei) proporcional ao seu cargo e nível de acesso a dados. As políticas também identificam as responsabilidades funcionais para a administração de acesso lógico e de segurança.

Provisionamento de conta

A responsabilidade pelo provisionamento do acesso do contratante e do funcionário é compartilhada entre

proprietários de serviço, operações corporativas e recursos humanos (RH).

Uma conta padrão do funcionário ou contratante com privilégios mínimos é configurada em um estado desabilitado quando um gerente contratante envia sua aprovação. A conta é ativada automaticamente quando o registro de funcionário é ativado no sistema de RH da Amazon.

O acesso a outros recursos, incluindo serviços, Hosts, dispositivos de rede, grupos Windows e UNIX deve ser explicitamente aprovado no sistema de gerenciamento de permissão do proprietário da Amazon por um proprietário ou gerente apropriado. Todas as alterações afetadas na ferramenta de gerenciamento de permissões são abordadas em uma auditoria. Quando ocorrem alterações em função do trabalho do funcionário, a continuidade de acesso deve ser explicitamente aprovada para o recurso ou será automaticamente revogada.

<u>Revisão de conta</u>
Cada concessão de acesso é revista a cada 90 dias; uma nova aprovação explícita é necessária ou o acesso ao recurso é revogado automaticamente.

<u>Exclusão de acesso</u>
O acesso é revogado automaticamente quando o registro de um funcionário é finalizado no sistema de recursos humanos da Amazon. As contas do Windows e UNIX são desabilitadas e o sistema de gerenciamento de permissão da Amazon remove o usuário de todos os sistemas.

<u>Política de senhas</u>
O acesso e a administração de segurança lógica para a Amazon depende de IDs de usuário, senhas Kerberos para autenticar usuários para serviços, recursos e dispositivos, bem como para autorizar o nível adequado de acesso para o usuário. A segurança AWS estabeleceu uma política de senha com intervalos de expiração e configurações necessárias.

Segurança física

A Amazon tem muitos anos de experiência no projeto, na construção e na operação de datacenters de grande escala. Esta experiência tem sido aplicada à plataforma e à infraestrutura da AWS. Os datacenters da AWS estão alojados em instalações inclassificáveis. O acesso físico é estritamente controlado no perímetro e nos pontos de ingresso de construção pelos funcionários da segurança profissional utilizando a vigilância por vídeo, sistemas de detecção de intrusão e outros meios eletrônicos. O pessoal autorizado deve passar pela autenticação de dois fatores por um mínimo de duas vezes para acessarem os andares dos datacenter. Todos os visitantes e prestadores de serviços estão obrigados a apresentar identificação e são cadastrados e continuamente escoltados por pessoal autorizado.

AWS só fornece acesso de datacenter e informações para funcionários e prestadores de serviços que têm uma empresa legítima necessidade de tais privilégios. Quando um funcionário não tem mais uma necessidade de negócio para estes privilégios, seu acesso é imediatamente revogado, mesmo se continuam a ser um funcionário da Amazon ou da Amazon Web Services. Todo o acesso físico aos datacenters por funcionários da AWS é registrado e auditado rotineiramente.

Proteções ambientais

Os centros de dados da Amazon são de última geração, utilizando abordagens inovadoras de arquitetura e de engenharia.

<u>Detecção de incêndio e supressão</u>
Equipamentos automáticos de detecção e supressão de fogo foram instalados para reduzir o risco. O sistema de detecção de incêndio utiliza sensores de detecção de fumaça em todos os ambientes do datacenter, espaços de

infraestrutura elétrica e mecânica, salas chiller e salas de equipamento gerador. Essas áreas são protegidas por sistemas de incêndio de tubos úmidos, interbloqueados duplos ou sistemas de aspersão gasosos.

Energia
Os sistemas de energia elétrica do datacenter sistemas são projetados para serem totalmente redundantes e passíveis de manutenção sem impacto para as operações, 24 horas por dia e sete dias por semana. As Unidades de Alimentação de Energia Ininterrupta (UPS) fornecem energia de apoio no caso de uma falha elétrica para cargas críticas e essenciais da empresa. Os datacenters usam geradores para fornecer energia para toda a instalação.

Clima e temperatura
O controle climático é necessário para manter uma temperatura operacional constante para servidores e outros hardware, o que impede o superaquecimento e reduz a possibilidade de interrupções do serviço. Os datacenters estão condicionados a manter condições atmosféricas em níveis ideais. Colaboradores e sistemas monitoram e controlam a temperatura e a umidade em níveis adequados.

Gerenciamento
A AWS monitora sistemas elétricos, mecânicos e de manutenção de funções vitais para que qualquer problema seja imediatamente identificado. A manutenção preventiva é executada para manter a operacionalidade contínua dos equipamentos.

Gerenciamento de configuração

Alterações de emergência, não rotineiras e outras alterações de configuração à infraestrutura existente da AWS são autorizadas, conectadas, testadas, aprovadas e documentadas em conformidade com as normas do setor para sistemas similares. Atualizações de infraestrutura da AWS são feitas para minimizar qualquer impacto sobre o cliente e seu uso dos serviços. A AWS se comunicará com os clientes via e-mail ou através do Console de status de serviço AWS (http://status.aws.amazon.com/) quando a utilização do serviço se tornar susceptível a situações negativas.

Software
A AWS aplica uma abordagem sistemática para o gerenciamento de mudanças para que alterações ao cliente que afetem os serviços sejam cuidadosamente revistas, testadas, aprovadas e bem comunicadas.

O processo de gerenciamento de alterações da AWS é projetado para evitar interrupções de serviço não intencionais e para manter a integridade do serviço ao cliente. As alterações implantadas nos ambientes de produção são:

- Revisadas: processo de revisão pelos pares dos aspectos técnicos de uma mudança
- Testadas: ao serem aplicadas se comportarão conforme o esperado e não impactarão negativamente o desempenho
- Aprovadas: para fornecer supervisão adequada e compreensão sobre o impacto nos negócios

Alterações são normalmente enviadas para produção em uma implantação em fases começando com áreas de menor impacto. As implantações são testadas em um único sistema e são monitoradas de perto para que o impacto possa ser avaliado. Os proprietários de serviço possuem várias métricas configuráveis que medem a integridade de dependências da produção do serviço. Essas métricas são rigorosamente monitoradas com os limites e alertas em vigor. Procedimentos de reversão estão documentados no ticket Change Management (CM).

Sempre que possível, as alterações são agendadas durante as janelas de alterações regulares. As alterações de emergência aos sistemas de produção que precisem de desvios dos procedimentos de gerenciamento de alteração padrão estão associadas a um incidente e são registradas e aprovadas conforme apropriado.

Periodicamente, a AWS realiza autoauditorias de alterações aos serviços chaves para controlar a qualidade, manter altos padrões e facilitar a melhoria contínua do processo de gestão de alterações. Todas as exceções são analisadas para determinar a causa raiz e assegurar que as ações apropriadas sejam tomadas para que a alteração esteja em conformidade ou para reverter a alteração se necessário. Ações são tomadas, em seguida, para abordar e corrigir o processo ou a emissão de pessoas.

Infraestrutura

A equipe de aplicativos corporativos da Amazon desenvolve e gerencia software para automatizar processos de TI para hosts UNIX/Linux nas áreas de distribuição de software de terceiros, software desenvolvido internamente e gerenciamento de configuração. A equipe de infraestrutura mantém e opera uma estrutura de gerenciamento de configuração UNIX/Linux para abordar o gerenciamento de escalabilidade, disponibilidade, auditoria e segurança de hardware. Gerenciando centralmente os hosts através da utilização de processos automatizados que gerenciam as alterações, a empresa é capaz de alcançar seus objetivos de alta disponibilidade, repetibilidade, escalabilidade, segurança robusta e recuperação de desastres. Os engenheiros de rede e de sistemas monitoram o status dessas ferramentas automatizadas diariamente, revendo relatórios para atender aos hosts que não conseguem obter ou atualizar seu software e sua configuração.

Um software de gerenciamento de configuração desenvolvido internamente é instalado quando o novo hardware é configurado. Essas ferramentas são executadas em todos os hosts UNIX para validar sua configuração e assegurar-se de que o software está instalado em conformidade com as normas determinadas pelo papel atribuído ao host. Este software de gerenciamento de configuração também ajuda a atualizar regularmente os pacotes que já estão instalados no host. Somente colaboradores habilitados pelas permissões de serviço podem fazer login em servidores de gerenciamento de configuração central.

Gerenciamento de continuidade de negócios

A infraestrutura da Amazon tem um elevado nível de disponibilidade os recursos para implantar uma arquitetura de TI resiliente. A AWS projetou seus sistemas para tolerar falhas do sistema ou de hardware impacto ao cliente. O gerenciamento de continuidade de negócios de datacenters da AWS está sob a direção do Grupo de Infraestrutura da Amazon.

Disponibilidade

Os datacenters são construídos em clusters em várias regiões globais. Todos os datacenters estão online e a serviço dos clientes; nenhum datacenter está "inativo". Em caso de falha, processos automatizados desviam o tráfego de dados do cliente da área afetada. Os principais aplicativos são implantados em uma configuração N + 1 , para que no caso de uma falha do datacenter, haja capacidade suficiente para permitir que o tráfego seja balanceado para os locais restantes.

A AWS oferece aos clientes a flexibilidade de alocar instâncias e armazenar dados em várias regiões geográficas, bem como em várias zonas de disponibilidade dentro de cada região. Cada Zona de disponibilidade é concebida como uma zona de falha independente. Isto significa que as Zonas de disponibilidade são fisicamente separadas dentro de uma região metropolitana específica e estão localizadas nas planícies de inundação de risco inferior (categorização de zona de inundação específica varia por região). Além de discretas fontes de alimentação ininterrupta (UPS) e instalações de geração de backup no local, cada uma é alimentada através de grades diferentes de utilitários independentes para reduzir ainda mais os pontos únicos de falha. Zonas de disponibilidade são todas redundantemente conectadas a vários provedores de trânsito de nível 1.

Os clientes devem projetar seu uso da AWS para tirar proveito de várias regiões e zonas de disponibilidade. A distribuição de aplicativos em várias zonas de disponibilidade fornece a capacidade de permanecer flexível diante da maioria dos modos de falha, incluindo catástrofes naturais ou falhas do sistema.

Resposta a incidentes
A equipe de gerenciamento de incidentes da Amazon emprega procedimentos de diagnóstico padrão do setor para impulsionar a resolução durante eventos que afetam os negócios. Os colaboradores operacionais fornecem apoio e suporte 24h x 7 dias x 365 dias para detectar incidentes e gerenciar o impacto e a resolução.

Análise de Executiva de toda a empresa
O grupo de auditoria interna da Amazon reviu recentemente os planos de resiliência de serviços AWS, que são também periodicamente revisados por membros da equipe de gerenciamento executivo sênior e pelo Comitê de auditoria do Conselho Administrativo.

Observe que em 21 de abril de 2011, o EC2 sofreu uma interrupção do serviço ao cliente afetando a região leste dos EUA. Detalhes sobre a interrupção do serviço são descritas no "Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region" (http://aws.amazon.com/message/65648/).

Backups

O Amazon S3 e o Amazon SimpleDB fornecem durabilidade do objeto ao armazenar os objetos várias vezes em várias zonas de disponibilidade na gravação inicial e, em seguida, ativamente fazendo ainda mais a replicação em caso de indisponibilidade do dispositivo ou detectado bit-rot. A replicação do Amazon EBS é armazenada dentro da mesma Zona de disponibilidade, não em várias zonas e, portanto, altamente recomenda que os clientes realizem instantâneos regulares para Amazon S3 para durabilidade de dados a longo prazo. A replicação do Amazon EBS é armazenada dentro da mesma Zona de disponibilidade, não em várias zonas e, portanto, altamente recomenda que os clientes realizem instantâneos regulares para Amazon S3 para durabilidade de dados a longo prazo. Para clientes que tenham projetado bancos de dados transacionais complexos usando o EBS, recomenda-se realizar backups no Amazon S3 através do sistema de gerenciamento de banco de dados para que os registros e as transações distribuídas possam ser verificados. A AWS não realiza backups de dados que são mantidos em discos virtuais conectados a instâncias em execução no Amazon EC2.

Desativação do dispositivo de armazenamento

Quando um dispositivo de armazenamento atingiu o final da sua vida útil, os procedimentos da AWS incluem um processo de desativação que é projetado para impedir que os dados do cliente sejam expostos a pessoas não autorizadas. A AWS usa as técnicas detalhadas no DoD 5220.22-M ("National Industrial Security programa Manual de utilização") ou NIST 800-88 ("orientações para o tratamento de mídia") para destruir dados como parte do processo de desativação. Se um dispositivo de hardware é incapaz de ser desativado usando esses procedimentos, o dispositivo será inutilizado ou fisicamente destruído em conformidade com as práticas padrão do setor.

Separação de falhas

A AWS oferece aos clientes a flexibilidade de alocar instâncias e armazenar dados em várias regiões geográficas. Cada região é uma coleção independente dos recursos AWS em uma localização geográfica definida. A AWS atualmente oferece suporte a cinco regiões: leste dos EUA (Virgínia do norte), oeste dos EUA (norte da Califórnia), UE (Irlanda), Ásia-Pacífico (Cingapura) e Pacífico Asiático (Tóquio). A região dos EUA padrão do Amazon S3 inclui instalações no leste dos EUA na Virgínia do Norte e no oeste do Estado de Washington.

A seleção de uma região dentro de uma jurisdição geográfica aceitável ao cliente fornece uma base sólida para atender aos requisitos de privacidade e de conformidade que dependem da localização, tais como a política de privacidade de dados da União Europeia. Os dados não são replicados entre regiões exceto se proativamente solicitado pelo cliente, permitindo que os clientes com esses tipos de localização de dados e requisitos de privacidade tenham a capacidade de

estabelecer ambientes compatíveis. Vale destacar que todas as comunicações entre as regiões ocorre através de uma infraestrutura de Internet pública. Métodos de criptografia apropriados devem ser usados para proteger dados confidenciais.

Dentro de uma determinada região, o Amazon EC2, o Amazon EBS e o Amazon Relational Database Service (RDS) permitem que os clientes aloquem instâncias e armazenem dados em várias Zonas de disponibilidade. Consulte a seção "Gerenciamento de continuidade de negócios" para obter mais informações sobre a disponibilidade.

O Amazon S3, o Amazon SimpleDB, o Amazon Simple Notification Service (SNS) e o Amazon Simple Queue Service (SQS) não expõem o conceito de Zonas de disponibilidade para os clientes. Com esses serviços, os dados são armazenados redundantemente em vários dispositivos de múltiplas instalações dentro de uma região.

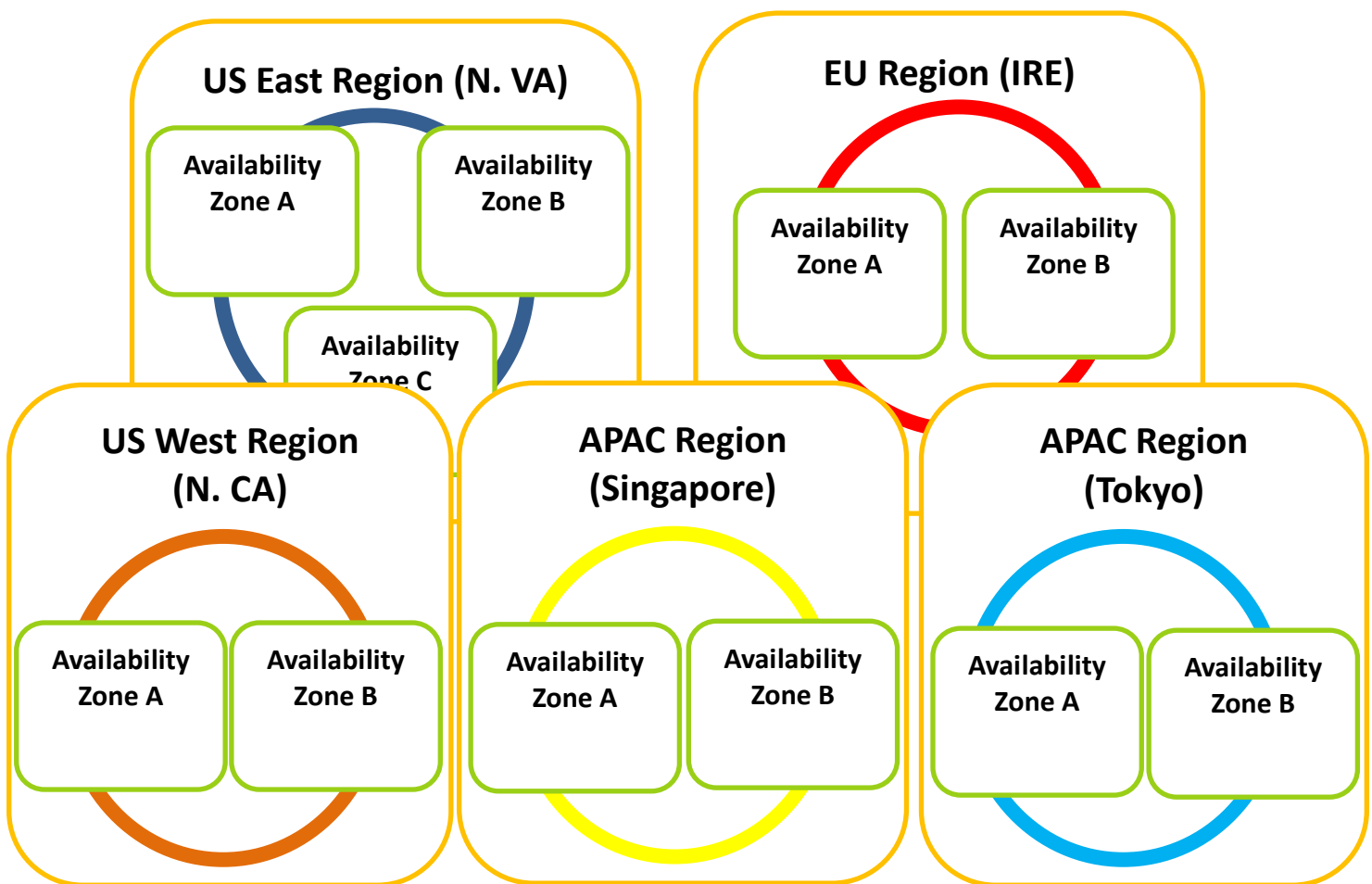
O diagrama abaixo demonstra as regiões e as Zonas de disponibilidade dentro de cada região para o Amazon EC2, o Amazon EBS e o Amazon RDS.

US East Region (N. VA)
Availability Zone A
Availability Zone B
Availability Zone C

EU Region (IRE)
Availability Zone A
Availability Zone B

US West Region (N. CA)
Availability Zone A
Availability Zone B

APAC Region (Singapore)
Availability Zone A
Availability Zone B

APAC Region (Tokyo)
Availability Zone A
Availability Zone B

Recursos de segurança de conta da Amazon

AWS fornece várias maneiras para que os clientes se identifiquem e acessem com segurança sua conta AWS. Uma lista completa de credenciais compatíveis com a AWS pode ser encontrada na página de credenciais de segurança em Sua conta. A AWS também fornece opções de segurança adicionais que permitem que os clientes protejam ainda mais as suas contas da AWS e controlem o acesso: Identity and Access Management (IAM), Multi-gateway de internet Authentication (MFA) e Rotação de chave da AWS.

AWS Identity and Access Management (AWS IAM)

O AWS Identity and Access Management (AWS IAM) permite que o cliente crie múltiplos usuários e gerencie permissões para cada um desses usuários a partir de sua conta da AWS. Um Usuário é uma identidade (dentro de uma conta da AWS do cliente) com credenciais de segurança exclusivas que podem ser usadas para acessar os serviços da AWS. O IAM da AWS elimina a necessidade de compartilhar senhas ou chaves de acesso e facilita a ativação e a desativação de um acesso do Usuário, conforme apropriado.

O IAM da AWS permite que o cliente implemente as melhores práticas de segurança, tais como menos privilégio, ao atribuir credenciais exclusivas para cada usuário dentro da sua conta da AWS e conceder somente as permissões que os usuários precisam a fim de acessar os recursos da AWS necessários para a realização do seu trabalho. Como padrão, o IAM da AWS é seguro; os novos usuários não têm de acessar os recursos da AWS até que permissões sejam explicitamente concedidas.

O IAM da AWS permite que os clientes minimizem o uso das suas credenciais de conta da AWS. Em vez disso, todas as interações com os Serviços e recursos da AWS devem ocorrer com as credenciais de segurança do Usuário do IAM. Mais informações sobre o Identity and Access Management da AWS (IAM da AWS) estão disponíveis no website da AWS: http://aws.amazon.com/iam/

AWS Multi-gateway de internet Authentication (AWS MFA)

A AWS Multi-gateway de internet Authentication (AWS MFA) é uma camada adicional de segurança que oferece um melhor controle das suas configurações de conta da AWS e a gestão dos Serviços e recursos registrados da AWS para a sua conta. Ao habilitar esse recurso de opção de identificação, o cliente necessitará fornecer um código de uso único de seis dígitos, além das suas credenciais de nome de usuário padrão e de senha antes que o acesso seja concedido às suas configurações da conta AWS ou aos recursos e serviços da AWS. O cliente obterá esse código de uso único a partir de um dispositivo de autenticação, que estará em sua posse. Isso é chamado de Autenticação Multi-gateway de internet porque dois fatores são verificados antes de o acesso ser concedido: os clientes precisarão fornecer seu nome de usuário (e-mail da Amazon no caso de uma conta AWS) e senha (o primeiro "fator": algo que você sabe) e o código preciso de seu dispositivo de autenticação (o segundo "fator": algo que você tem). Os clientes podem ativar dispositivos MFA para suas contas da AWS, bem como para os usuários criados em contas da AWS com o IAM da AWS.

É fácil adquirir um dispositivo de autenticação de fornecedores terceirizados conveniados e configurá-lo para uso pelo site da Web da AWS. Mais informações sobre a Autenticação Multi-gateway de internet estão disponíveis no website da AWS: http://aws.amazon.com/mfa/

Rotação de chave

Pelos mesmos motivos que tornam importante a alteração de senhas frequentemente, a AWS recomenda que os clientes façam regularmente a rotação das suas chaves de acesso e certificados. Para permitir que o cliente possa fazer isso sem um possível impacto na disponibilidade dos seus aplicativos, a AWS é compatível com várias chaves de acesso e certificados simultâneos. Com esse recurso, os clientes podem fazer a rotação das chaves e certificados dentro e fora de operação de modo regular, sem qualquer tempo de inatividade para o seu aplicativo. Ele pode ajudar a diminuir os riscos de perda ou comprometimento de certificados ou chaves de acesso. As APIs do IAM da AWS permitem que o cliente faça a rotação das chaves de acesso da sua Conta da AWS, bem como para usuários criados sob a sua Conta da AWS usando o IAM da AWS.

Segurança de rede

A rede AWS fornece proteção significativa contra problemas de segurança de rede tradicional e o cliente pode

implementar mais proteção. A seguir alguns exemplos:

Ataques distribuídos de negação de serviço (DDoS)
Pontos de acesso de Application Programming Interface (API) da AWS são hospedados em uma infraestrutura grande, em escala de Internet e de classe mundial que se beneficia da mesma experiência em engenharia que fez da Amazon a maior varejista on-line do mundo. São usadas técnicas de redução de DDoS proprietárias. Além disso, as redes da AWS tem hospedagem múltipla através de vários provedores para alcançar a diversidade de acesso à Internet.

Ataques a intermediários (MITM)
Todas as APIs da AWS estão disponíveis através de pontos de acesso protegidos por SSL que fornecem autenticação de servidor. As AMIs do Amazon EC2 automaticamente geram novos certificados de host SSH na primeira inicialização e os registram no console da instância. Os clientes, em seguida, podem usar as APIs seguras para chamar o console e acessar os certificados de host antes de fazer o login na instância pela primeira vez. Os clientes são incentivados a usar o SSL para todas as suas interações com a AWS.

IP Spoofing
As instâncias Amazon EC2 não podem enviar tráfego de rede falsificado. A infraestrutura de firewall baseada em host controlada pela AWS não permitirá que uma instância envie tráfego com uma fonte de IP ou endereço MAC diferente do seu.

Varredura de Porta
Varreduras de portas não autorizadas pelos clientes do Amazon EC2 são uma violação da política de uso aceitável da AWS. Violações da política de uso aceitável AWS são levadas a sério, e cada violação relatada é investigada. Os clientes podem relatar abuso suspeito através dos contatos disponíveis em nosso website em: http://aws.amazon.com/contact-us/report-abuse/ Quando uma varredura de porta não autorizada é detectada ela é interrompida e bloqueada. As varreduras de portas de instâncias do Amazon EC2 são geralmente ineficazes, porque, por padrão, todas as portas de entrada nas instâncias do Amazon EC2 estão fechadas e só são abertas pelo cliente. O gerenciamento rigoroso do cliente de grupos de segurança pode atenuar ainda mais a ameaça de varreduras de portas. Se o cliente configura o grupo de segurança para permitir o tráfego de qualquer fonte para uma porta específica, essa porta específica ficará vulnerável a uma varredura de portas. Nestes casos, o cliente deve usar medidas de segurança adequadas para proteger os serviços de escuta que podem ser essenciais para que seu aplicativo não seja descoberto por uma varredura de portas não autorizada. Por exemplo, um servidor web deve ter a porta 80 (HTTP) aberta ao mundo, e o administrador deste servidor é responsável pela segurança do software do servidor HTTP, como o Apache. Os clientes podemsolicitar permissão para conduzir análises de vulnerabilidade conforme necessário para atender aos requisitos de conformidade específicos. Estas análises devem ser limitadas às instâncias do cliente e não devem violar a política de uso aceitável da AWS. A aprovação avançada para esses tipos de varreduras pode ser iniciada pelo envio de uma solicitação através do website em: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

Packet sniffing por outros clientes
Uma instância virtual que esteja sendo executada em modo promíscuo não pode receber ou "farejar" o tráfego que se destina a uma instância virtual diferente. Mesmo que os clientes possam colocar suas interfaces em modo promíscuo, o hypervisor não disponibilizará nenhum tráfego que não seja endereçado a eles. Mesmo duas instâncias virtuais que são pertencentes ao mesmo cliente localizado no mesmo host físico não podem escutar tráfego umas das outras. Ataques como envenenamento de cache ARP não funcionam no Amazon EC2 e no Amazon VPC. Enquanto o Amazon EC2 não oferece proteção ampla contra a tentativa mal-intencionada de um cliente de ver dados de outro, como uma prática padrão, todos os clientes devem criptografar o tráfego sensível.

Segurança do Amazon Elastic Compute Cloud (Amazon EC2)

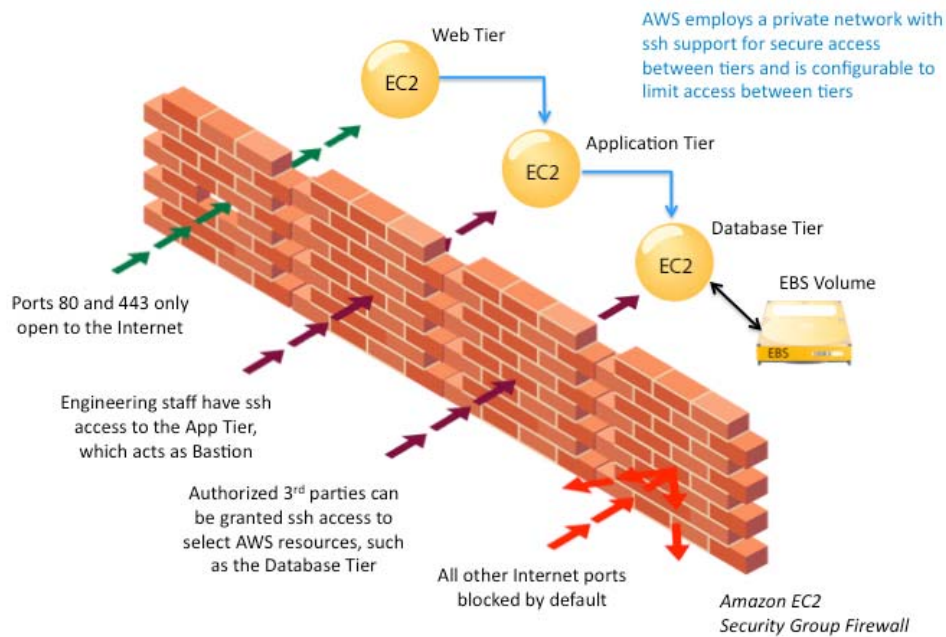
A segurança no Amazon EC2 é fornecida em vários níveis: o sistema operacional (SO) do sistema host, o sistema operacional da instância virtual ou sistema operacional convidado, um firewall e chamadas de API assinadas. Cada um desses itens amplia os recursos dos outros. O objetivo é oferecer proteção para que dados contidos no Amazon EC2 não sejam interceptados por sistemas ou usuários não autorizados e possam eles mesmos fornecer instâncias do Amazon EC2 que sejam tão seguras quanto possível sem sacrificar a flexibilidade na configuração que os clientes exigem.

Múltiplos Níveis de Segurança

Sistema operacional do host: os administradores com uma necessidade de negócios de acessar o plano de gerenciamento são solicitados a usar a autenticação multi-gateway de internet para obter acesso aos hosts de uso específico de administração. Esses hosts administrativos são sistemas que são especificamente concebidos, construídos, configurados e reforçados para proteger o plano de gestão da nuvem. Esse acesso é registrado e auditado. Quando um funcionário não tem mais uma necessidade de negócio para acessar o plano de gestão, os privilégios e o acesso a esses hosts e sistemas pertinentes são revogados.

Sistema operacional convidado: instâncias virtuais são totalmente controladas pelo cliente. Os clientes têm acesso completo à raiz ou controle administrativo sobre aplicativos, serviços e contas. A AWS não têm quaisquer direitos de acesso para instâncias de cliente e não podem efetuar login no sistema operacional convidado. A AWS recomenda um conjunto básico de melhores práticas de segurança recomendados para incluir a desativação do acesso somente por senha para seus hosts e da utilização de alguma forma de autenticação multi-factor para obter acesso as suas instâncias (ou a um mínimo acesso SSH versão 2 com base em certificado). Além disso, os clientes devem empregar um mecanismo de escalonamento de privilégio com registro em uma base por usuário. Por exemplo, se o sistema operacional convidado for Linux, depois de sua instância de proteção, eles devem utilizar SSHv2 com base em certificado para acessar a instância virtual, desativar o login remoto da raiz, usar o log de linha de comando e usar 'sudo' para a escalação de privilégios. Os clientes devem gerar seus próprios pares de chaves para garantir que sejam únicos e não compartilhados com outros clientes ou com a AWS.

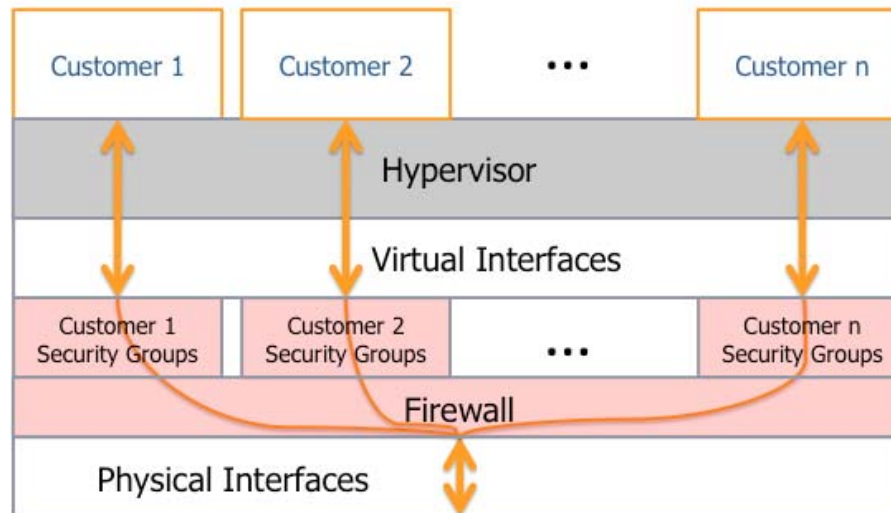
Firewall: o Amazon EC2 fornece uma solução de firewall completa; este firewall de entrada obrigatório é configurado no modo padrão de negar tudo e os clientes do Amazon EC2 devem explicitamente abrir as portas necessárias para permitir o tráfego de entrada. O tráfego pode ser restrito por protocolo, por porta de serviço, bem como por endereço IP de origem (bloco IP ou roteamento sem classe entre domíniosCIDR).

O firewall pode ser configurado em grupos permitindo que classes diferentes de instâncias tenham regras diferentes. Considere, por exemplo, o caso de um aplicativo web tradicional de três níveis. O grupo para os servidores web teria a porta 80 (HTTP) e/ou a porta 443 (HTTPS) aberta para a Internet. O grupo para os servidores de aplicativos teria a porta 8000 (específico do aplicativo) acessível somente para o grupo de servidor web. O grupo para os servidores de banco de dados teria a porta 3306 (MySQL) aberta apenas para o grupo de servidor de aplicativo. Todos os três grupos permitiriam o acesso administrativo na porta 22 (SSH), mas apenas a partir da rede corporativa do cliente. Aplicativos altamente seguros podem ser implantados usando esse mecanismo expressivo. Veja o diagrama abaixo:

O firewall não é controlado através de OS convidado; em vez disso, exige o certificado X.509 do cliente e chave para autorizar alterações, acrescentando assim uma camada extra de segurança. A AWS pode conceder acesso granular para diferentes funções administrativas sobre as instâncias e o firewall, portanto, que permita ao cliente implementar segurança adicional através da separação de funções. O nível de segurança proporcionado pelo firewall é uma função de quais portas são abertas pelo cliente e para que finalidade e duração. O estado padrão é negar todo o tráfego de entrada e os clientes devem planejar cuidadosamente o que será aberto quando criarem e protegerem os seus aplicativos. O gerenciamento de tráfego instruído e o design de segurança ainda são necessários em uma base por instância. A AWS ainda incentiva os clientes a aplicarem filtros adicionais por instância com firewalls baseados em host como IPtables ou o Firewall do Windows e VPNs. Isto pode restringir tanto o tráfego de entrada quanto o de saída em cada instância. Chamadas de API para iniciar e encerrar instâncias, alterar parâmetros de firewall e executar outras funções são assinadas pela chave de acesso secreto do cliente da Amazon, que poderia ser qualquer chave de acesso secreto das contas da AWS ou a chave de acesso secreto de um usuário criado com o IAM da AWS. Sem o acesso à chave de acesso secreto do cliente, as chamadas de API da Amazon EC2 não podem ser realizadas em seu nome. Além disso, as chamadas de API podem ser criptografadas com o SSL para manter a confidencialidade. A Amazon sempre recomenda o uso de pontos de acesso de API protegidos por SSL. O IAM da AWS também permite que um cliente possa controlar quais APIs criadas por um usuário no IAM da AWS terão permissão para chamar.

O hypervisor

O Amazon EC2 utiliza atualmente uma versão personalizada do Xen hypervisor. Visto que os convidados paravirtualizados dependem do hypervisor para fornecer suporte para as operações que normalmente requerem um acesso privilegiado, o SO convidado não tem acesso elevado à CPU. A CPU fornece quatro modos de privilégio separados: 0-3, chamados de *anéis*. Sendo o anel 0 o mais privilegiado e o 3 o menos privilegiado. O SO host é executado em anel 0. No entanto, em vez de ser executado no anel 0 como a maioria dos sistemas operacionais, o SO convidado é executado em um anel 1 menos privilegiado e os aplicativos são executados em um menos privilegiado anel 3. Esta virtualização explícita dos recursos físicos leva a uma separação clara entre convidado e hypervisor, resultando na separação de segurança adicional entre os dois.

Isolamento de instância

Diferentes instâncias em execução na mesma máquina física são isoladas umas das outras, através do hypervisor Xen. A Amazon é ativa participante da comunidade Xen, o que garante o emprego dos últimos desenvolvimentos. Além disso, o firewall AWS reside na camada hypervisor, entre a interface de rede física e a interface da instância virtual. Todos os pacotes devem passar por esta camada, assim, uma instância vizinha não têm mais acesso a essa instância do que qualquer outro host na Internet e pode ser tratada como se eles estivessem em hosts físicos separados. A memória RAM é separada com mecanismos similares.

Instâncias do cliente não têm acesso a dispositivos de disco, mas são apresentadas como discos virtuais. A camada de virtualização de propriedade de disco da AWS, automaticamente redefine cada bloco de armazenamento utilizado pelo cliente, garantindo que os dados de um cliente nunca são involuntariamente expostos a outro. A AWS recomenda que os clientes protejam seus dados através de meios adequados. Uma solução comum é executar um arquivo criptografado no topo do dispositivo de disco virtual.

Segurança do Elastic Block Storage (Amazon EBS)

O acesso ao volume Amazon EBS é restrito para a conta da AWS que criou o volume e para os usuários sob a conta da AWS criada com o IAM da AWS se o usuário tiver concedido o acesso às operações EBS, negando assim a permissão para todas as outras contas e usuários da AWS para exibir ou acessar o volume. No entanto, um cliente pode criar snapshots Amazon S3 do seu volume Amazon EBS e habilitar outras contas da AWS para serem capacitadas a utilizar o snapshot compartilhado como base para a criação de seus próprios volumes. Os clientes também são habilitados a fazer snapshots do volume Amazon EBS publicamente disponível para todas as contas da AWS. O compartilhamento de snapshots do volume Amazon EBS não fornece outras contas da AWS com a permissão para alterar ou excluir o snapshot original ja que esse direito é explicitamente reservado para a conta da AWS que criou o volume. Um snapshot do EBS é uma visualização do nível de bloco de um volume EBS inteiro. Os dados que não são visíveis através do sistema de arquivos no volume, tais como arquivos que foram excluídos, podem estar presentes no snapshot do EBS. Os clientes que desejam criar snapshots compartilhados devem fazê-lo com cuidado. Se um volume continha dados confidenciais ou arquivos excluídos, um novo volume do EBS deve ser criado. Os dados que serão armazenados no snapshot compartilhado devem ser copiados para o novo volume e o snapshot criado a partir do novo volume.

Os volumes do Amazon EBS são apresentados ao cliente como dispositivos em bloco não formatado bruto, que foram eliminados antes de serem disponibilizadas para uso. Os clientes que têm procedimentos que exigem que todos os dados sejam eliminados através de um método específico, tais como as detalhadas no DoD 5220.22-M ("National

Industrial Security programa Manual de utilização") ou NIST 800-88 ("orientações para o tratamento de mídia"), têm a capacidade de fazê-lo no Amazon EBS. A criptografia de dados confidenciais geralmente é uma boa prática de segurança, e a AWS incentiva os usuários a criptografarem seus dados confidenciais através de um algoritmo coerente com sua política de segurança definida.

Segurança do Amazon Virtual Private Cloud

A segurança dentro do Amazon Virtual Private Cloud começa com o próprio conceito de VPC e se estende para incluir os grupos de segurança, listas de controle de acesso de rede (ACLs), roteamento e gateways externos. Cada um desses itens é complementar ao fornecer uma rede isolada e segura, que pode ser estendida por meio da habilitação seletiva do acesso direto à Internet ou conectividade privada para outra rede. Abaixo descrevemos os vários níveis de segurança do Amazon VPC. Isso será seguido por um diagrama que ilustra como os componentes do Amazon VPC se relacionam.

Múltiplos Níveis de Segurança

Virtual Private Cloud: Cada VPC é uma rede distinta, isolada dentro da nuvem. No momento da criação, um intervalo de endereços IP para cada VPC é selecionado pelo cliente. O tráfego de rede dentro de cada VPC é isolado de todos os outros VPCs; portanto, vários VPCs podem utilizar a sobreposição de intervalos de endereços IP (mesmo idênticos) sem perda desse isolamento. Por padrão, os VPCs não possuem conectividade externa. Os clientes podem criar e anexar um gateway de internet, gateway VPN ou ambos para estabelecer uma conectividade externa, sujeitos aos controles abaixo.

API: chamadas para criar e excluir VPCs, alteração de roteamento, grupo de segurança, parâmetros de rede ACL e executar outras funções são assinadas pela chave secreta de acesso do cliente da Amazon, que poderia ser qualquer chave secreta de acesso das contas da AWS ou a chave secreta de acesso de um usuário criado com o IAM da AWS. Sem o acesso à chave secreta de acesso do cliente, as chamadas de API da Amazon VPC não podem ser realizadas em nome do cliente. Além disso, as chamadas de API podem ser criptografadas com o SSL para manter a confidencialidade. A Amazon sempre recomenda o uso de pontos de acesso de API protegidos por SSL. O IAM da AWS também permite que um cliente possa controlar quais APIs um usuário recém-criado terá permissão para chamar.

Sub-redes: os clientes criam uma ou mais sub-redes dentro de cada VPC; cada instância lançada no VPC é conectada a uma sub-rede. Traditional Layer 2 security attacks, including MAC spoofing and ARP spoofing, are blocked.

Tabelas de rota e rotas: cada sub-rede em um VPC é associada a uma tabela de roteamento e todo o tráfego de rede saindo de uma sub-rede é processado pela tabela de roteamento para determinar o destino.

Gateway VPN: um gateway VPN permite conectividade privada entre o VPC e outra rede. O tráfego de rede dentro de cada gateway VPN é isolado do tráfego de rede dentro de todos os outros gateways de VPN. Os clientes podem estabelecer conexões VPN para o gateway VPN de dispositivos de gateway do cliente. Cada conexão é protegida por uma chave pré-compartilhada em conjunto com o endereço de IP do dispositivo de gateway do cliente.

Gateway de internet: um gateway de internet pode ser ligado ao VPC para permitir a ligação direta com a Amazon S3, outros serviços AWS e a Internet. Cada instância que deseja esse acesso deve ter um IP elástico associado a ela ou rotear o tráfego por meio de uma instância NAT. Além disso, as rotas de rede estão configuradas (ver acima) para direcionar o tráfego para o gateway de internet. A AWS fornece referência AMIs de NAT que podem ser extendidas pelos clientes para realizar o registro de rede, inspeção profunda de pacotes, filtragem de camada de aplicativo ou outros controles de segurança.

Este acesso só pode ser modificado através da chamada de APIs do Amazon VPC. A AWS pode conceder acesso granular para diferentes funções administrativas sobre as instâncias e o gateway de internet, portanto, que permita ao cliente implementar segurança adicional através da separação de funções.

Instâncias do Amazon EC2: as instâncias do Amazon EC2 em execução com o Amazon VPC contêm todos os benefícios descritos acima relacionados com o sistema operacional do host, sistema operacional convidado, hypervisor, instância de isolamento e pacote de proteção contra detecção.

Locação: um VPC permite que os clientes iniciem as instâncias do Amazon EC2 que são fisicamente isoladas em·nível de hardware de host; elas serão executadas em um hardware de locação única. Um VPC pode ser criado com locação 'dedicada', nesse caso todas as instâncias lançadas para o VPC vão utilizar esse recurso. Alternatively, a VPC may be created with ‘default’ tenancy, but customers may specify ‘dedicated’ tenancy for particular instances launched into the VPC.

Firewall (grupos de segurança): como o Amazon EC2, o Amazon VPC oferece suporte uma solução de firewall completa para ativar a filtragem de tráfego de entrada e saída de uma instância. O grupo padrão permite a comunicação de entrada de outros membros do mesmo grupo e comunicação de saída para qualquer destino. O tráfego pode ser restrito por qualquer protocolo IP, pela porta de serviço, bem como endereço de IP de origem/destino (bloco de IP ou roteamento sem classe entre domínios (CIDR) individual).

O firewall não é controlado através de SO convidado; pelo contrário, ele pode ser modificado somente através da chamada de APIs do Amazon VPC. A AWS pode conceder acesso granular para diferentes funções administrativas sobre as instâncias e o firewall, portanto, que permita ao cliente implementar segurança adicional através da separação de funções. O nível de segurança proporcionado pelo firewall é uma função de quais portas são abertas pelo cliente e para que finalidade e duração. O gerenciamento de tráfego instruído e o design de segurança ainda são necessários em uma base por instância. A AWS ainda incentiva os clientes a aplicarem filtros adicionais por instância com firewalls baseados em host como IPtables ou o Firewall do Windows.

Listas de controle de acesso de rede: para adicionar uma camada adicional de segurança dentro do Amazom VPC, os clientes podem configurar as ACLs de rede. Estes são filtros de tráfego sem monitoração de estado que se aplicam a todo o tráfego de entrada ou de saída de uma sub-rede no VPC. Essas ACLs podem conter regras ordenadas para permitir ou negar o tráfego com base em protocolo de IP, pela porta de serviço, bem como endereço de IP de origem/destino.

Como grupos de segurança, as redes ACLs são gerenciadas por meio de APIs do Amazon VPC, adicionando uma camada de proteção extra e habilitando esta segurança extra através da separação de funções.

Resumo de segurança de rede

O diagrama abaixo mostra de que maneira os controles de segurança citados acima se inter-relacionam para habilitar topologias de rede flexível, proporcionando o controle total sobre os fluxos de tráfego de rede.

VPC 10.0.0.0/16

Instance 1 10.0.0.6
Instance 2 10.0.0.7
Instance 3 10.0.10.9

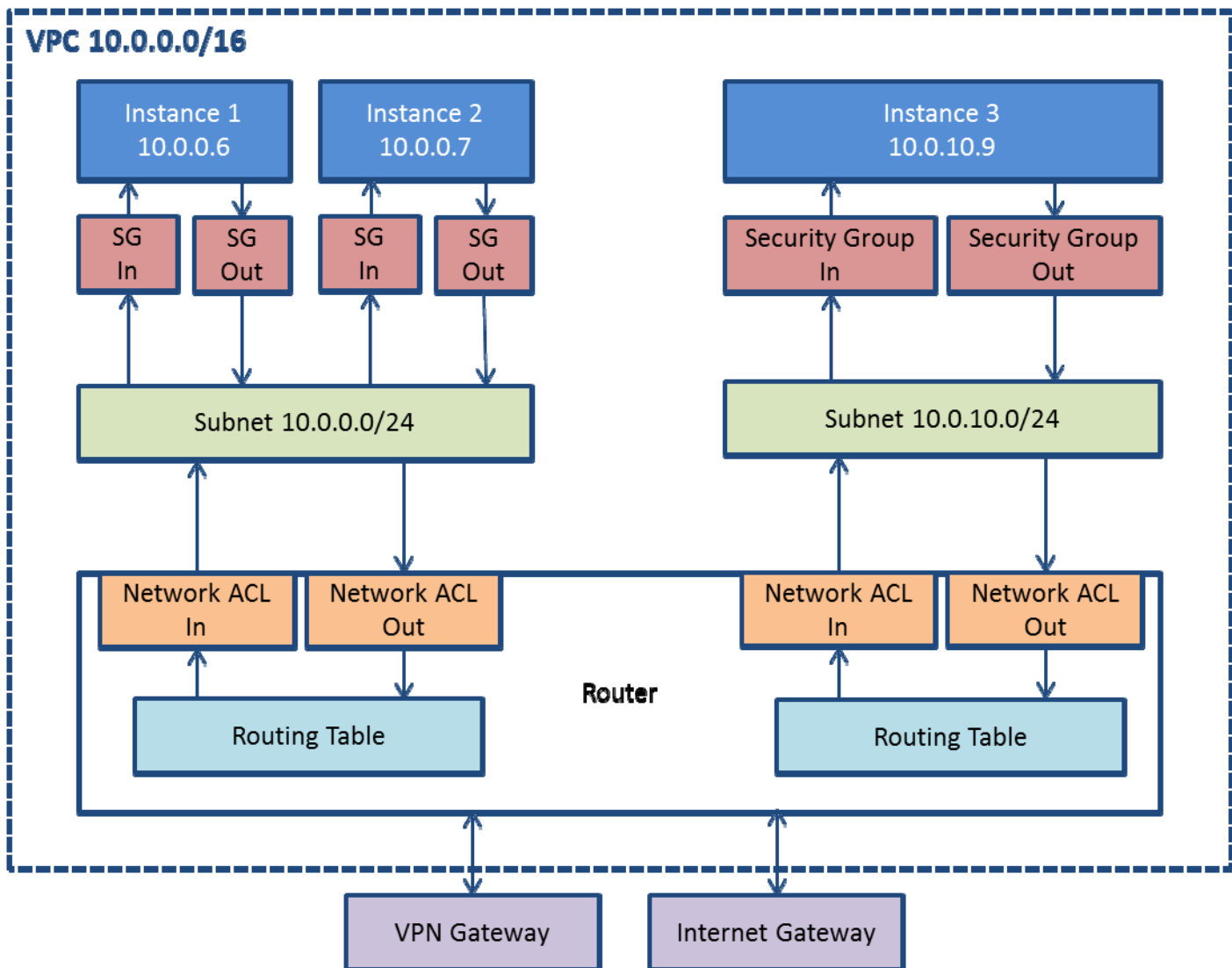
SG In
SG Out
SG In
SG Out
Security Group In
Security Group Out

Subnet 10.0.0.0/24
Subnet 10.0.10.0/24

Network ACL In
Network ACL Out
Network ACL In
Network ACL Out

Router

Routing Table
Routing Table

VPN Gateway
Internet Gateway

Segurança do Amazon Simple Storage Service (Amazon S3

Com qualquer sistema de armazenamento compartilhado, a questão de segurança mais comum é se os usuários não autorizados podem acessar as informações, intencionalmente ou por engano. Para garantir que os clientes possam ter flexibilidade para determinar como, quando e para quem deseja expor o armazenamento de informações na AWS, os APIs do Amazon S3 fornecem tanto os controles para acessar o nível de bucket e objeto, como também padrões que permitem apenas o acesso autenticado pelo criador do bucket e/ou objeto. A menos que um cliente conceda acesso anônimo aos seus dados, o primeiro passo antes de um usuário, tanto de uma conta AWS ou um usuário criado com o IAM da AWS, poder acessar os dados, é fazer a autenticação usando uma assinatura HMAC-SHA1 do pedido, utilizando a chave privada do usuário. Um usuário autenticado pode ler um único objeto, se tiver sido concedida permissão de leitura em uma Lista de Controle de Acesso (ACL) em nível de objeto. Um usuário autenticado pode listar as chaves e criar ou substituir os objetos em um bucket somente se tiver sido concedida a permissão de ler e escrever em uma ACL em nível bucket ou através de permissões concedidas a ele com o IAM da AWS. O nível ACLs do bucket e do objeto são independentes; um objeto não herda ACLs de seu bucket. As permissões para ler ou modificar o bucket ou o objeto ACLs são controladas por ACLs padrão para que somente o criador tenha acesso. Portanto, o cliente mantém total controle sobre quem tem acesso aos seus dados. Os clientes podem conceder acesso aos seus dados do Amazon S3 para outras contas da AWS pelo ID da conta da AWS ou e-mail, ou ainda pelo ID do produto DevPay. Os clientes também podem

conceder acesso aos seus dados do Amazon S3 para todas as contas da AWS ou para todos (ativando o acesso anônimo).

Gerenciamento de dados

Para máxima segurança, o Amazon S3 é acessível através de pontos de acesso com SSL. Os pontos de acesso criptografados são acessíveis a partir da Internet e de dentro do Amazon EC2, assegurando que os dados sejam transferidos de forma segura, tanto dentro da AWS como para locais externos.

Proteger dados envolve a segurança física e a criptografia dos dados. Como mencionado detalhadamente em "Segurança física", a Amazon emprega várias medidas de segurança física para proteger os dados em repouso do cliente. Por exemplo, o acesso físico dos datacenters da Amazon é limitado a uma lista auditada dos colaboradores da Amazon. A criptografia de dados confidenciais geralmente é uma boa prática de segurança e a AWS incentiva os usuários a criptografar seus dados confidenciais antes que eles sejam carregados para o Amazon S3.

Quando um objeto é excluído do Amazon S3, a remoção do mapeamento do nome público para o objeto começa imediatamente, e geralmente é processado através da distribuição sistemática dentro de alguns segundos. Uma vez que o mapeamento é removido, não há acesso remoto para o objeto excluído. A área de armazenamento subjacente é recuperada em seguida, para utilização pelo sistema.

O Amazon S3 é projetado para fornecer uma durabilidade de 99,999999999% e uma disponibilidade de 99.99% de objetos durante um determinado ano. Os objetos são armazenados redundantemente em vários dispositivos em diversas instalações em uma região do Amazon S3. Para ajudar a assegurar a durabilidade, as operações PUT e do Amazon S3 armazenam de forma sincronizada os dados em diversas instalações antes de exibir o SUCCESS. Uma vez armazenados, o Amazon S3 mantém a durabilidade dos objetos ao detectar e reparar rapidamente qualquer redundância perdida. O Amazon S3 também verifica regularmente a integridade dos dados armazenados usando somatórias. Se um corrompimento for detectado, ele será reparado usando dados redundantes. Além disso, o Amazon S3 calcula somatórias em todo o tráfego da rede para detectar o corrompimento de pacotes de dados durante a classificação ou a recuperação de dados.

O Amazon S3 fornece mais proteção via Versioning. O Versioning pode ser usado para preservar, recuperar e restaurar todoas as versões de todos os objetos armazenados no balde do Amazon S3. Com o Versioning é possível que você se recupere facilmente de ações não intencionais do usuário e de falhas do aplicativo. Como padrão, as solicitações recuperarão a versão gravada mais recente. As versões mais antigas de um objeto podem ser recuperadas especificando-se uma versão na solicitação. Você pode proteger ainda mais suas versões usando o recurso Amazon S3 Versioning's MFA Delete, uma vez habilitado para um bucket S3, cada solicitação de exclusão de versão deve incluir um código de seis dígitos e número de série do seu dispositivo de autenticação multi-factor.

Registro de acesso

Um bucket do Amazon S3 pode ser configurado para acessar o log do bucket e os objetos que estão dentro dele. O log de acesso contém detalhes sobre cada solicitação de acesso, incluindo o tipo de solicitação, o recurso solicitado, IP do solicitante e a hora e data do pedido. Quando o registro é habilitado para um bucket, as gravações de log são periodicamente agregadas em arquivos de log e entregues para o bucket do Amazon S3 especificado.

Segurança do Amazon Simple Data Base (SimpleDB)

As APIs do Amazon SimpleDB fornecem controles em nível de domínio que só permitem acesso autenticado pelo criador do domínio, por conseguinte, o cliente mantém total controle sobre quem tem acesso aos seus dados.

O acesso ao Amazon SimpleDB pode ser concedido com base em uma identificação de conta AWS. Uma vez autenticada, a conta AWS tem acesso completo a todas as operações. O acesso a cada domínio individual é controlado por uma lista

de controle de acesso independente que mapeia usuários para os domínios que possuem autenticação. Um usuário criado com o IAM da AWS só tem acesso às operações e aos domínios para os quais teve permissão concedida através da política.

O Amazon SimpleDB é acessível através de pontos de acesso criptografados com SSL. Os pontos de acesso criptografados são acessíveis tanto pela Internet quanto pelo Amazon EC2. Os dados armazenados dentro do Amazon SimpleDB não são criptografados pela AWS; no entanto o cliente pode criptografar os dados antes de carregá-los para o Amazon SimpleDB. Estes atributos criptografados seriam recuperáveis como parte de uma operação Get apenas. Eles não poderiam ser usados como parte de uma consulta de condição de filtragem. Criptografar os dados antes de enviá-los para o Amazon SimpleDB ajuda a proteger contra o acesso por qualquer pessoa aos dados confidenciais do cliente, incluindo a AWS.

Gerenciamento de dados do Amazon SimpleDB

Quando um domínio é excluído do Amazon SimpleDB, a remoção de mapeamento de domínio começa imediatamente e geralmente é processada em todo o sistema distribuído em poucos segundos. Uma vez que o mapeamento é removido, não há acesso remoto para os domínios excluídos.

Quando os dados de item e atributo são excluídos dentro de um domínio, a remoção de mapeamento dentro do domínio começa imediatamente e geralmente termina em segundos. Uma vez que o mapeamento é removido, não há acesso remoto para os dados excluídos. Essa área de armazenamento, em seguida, é disponibilizada apenas para operações de gravação e os dados são substituídos por dados armazenados recentemente.

Segurança do Amazon Relational Database Service (Amazon RDS)

O Amazon RDS permite que você crie rapidamente uma instância de banco de dados relacional, flexibilidade de escala associadas a recursos de computação e capacidade de armazenamento para atender à demanda de aplicativo. O Amazon RDS gerencia a instância de banco de dados em seu nome pela realização de backups, manipulação de failover e manutenção do software de banco de dados.

O acesso à instância de banco de dados do Amazon RDS é controlado pelo cliente através de grupos de segurança do banco de dados que são semelhantes a grupos de segurança do Amazon EC2, mas não são intercambiáveis. O padrão de grupos de segurança do banco de dados para um modo de acesso "negar todos" e os clientes devem autorizar especificamente o ingresso de rede. Há duas maneiras de fazer isso: autorizar um intervalo de IP de rede ou autorizar um grupo existente no Amazon EC2 Security Group. Os grupos de segurança do banco de dados só permitem o acesso à porta do servidor de banco de dados (todos os outros são bloqueados) e podem ser atualizados sem reiniciar a instância de banco de dados do Amazon RDS, o que permite que um cliente mantenha um controle contínuo do seu acesso de banco de dados.

Com o IAM da AWS um cliente ainda pode controlar o acesso a suas instâncias instância de banco de dados do RDS. O IAM da AWS permite que um cliente controle quais operações RDS cada usuário IAM da AWS tem permissão para chamar.

O Amazon RDS gera um certificado SSL para cada instância de banco de dados, permitindo que os clientes criptografem suas conexões de instância de banco de dados para aumentar a segurança.

Uma vez que a API de exclusão (DeleteDBInstance) de instância de banco de dados do Amazon RDS estiver em execução, a instância de banco de dados estará marcada para exclusão e assim que a instância não mais indicar o status "exclusão", ela terá sido removida. Neste momento a instância não está mais acessível e a menos que uma cópia de snapshot final tenha sido solicitada, ela não pode ser restaurada e não será listada por qualquer uma das ferramentas ou

APIs.

Segurança do Amazon Simple Queue Service (Amazon SQS)

O Amazon SQS é um serviço de enfileiramento de mensagens altamente confiável e escalável que permite a comunicação assíncrona baseada em mensagens entre os componentes distribuídos de um aplicativo. Os componentes podem ser computadores ou instâncias do Amazon EC2 ou uma combinação de ambos. Com o Amazon SQS você pode enviar um número qualquer de mensagens para uma fila do Amazon SQS a qualquer momento de qualquer componente. As mensagens podem ser obtidas através do mesmo componente ou um diferente, imediatamente ou em um momento posterior (no prazo de 4 dias). As mensagens são altamente duráveis; cada mensagem é armazenada constantemente em filas altamente disponíveis e altamente confiáveis. Vários processos podem ler/escrever de/para uma fila do Amazon SQS ao mesmo tempo sem interferir uns com os outros.

O acesso ao Amazon SQS é concedido com base em uma conta AWS ou um usuário criado com o IAM AWS. Uma vez autenticada, a conta AWS tem acesso completo a todas as operações do usuário. No entanto, um usuário IAM AWS só tem acesso às operações e a filas que tenham sido concedidas o acesso por via política. Por padrão, o acesso para cada fila individual é restrito para a conta AWS que o criou. No entanto, um cliente pode permitir que outros acessem uma fila, usando uma política gerada pelo SQS ou uma política escrita pelo usuário.

O Amazon SQS é acessível através de pontos de acesso criptografados com SSL. Os pontos de acesso criptografados são acessíveis tanto pela Internet quanto pelo Amazon EC2. Os dados armazenados no Amazon SQS não são criptografados pela AWS; no entanto o usuário pode criptografar dados antes carregá-los para o Amazon SQS, desde que o aplicativo utilizado pela fila possa descriptografar a mensagem quando os dados forem recuperados. Criptografar as mensagens antes de enviá-las para o Amazon SQS ajuda a proteger contra o acesso não autorizado aos dados confidenciais do cliente, incluindo a AWS.

Segurança do Amazon Simple Notification Service (Amazon SNS)

O Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que facilita a configuração, a operação e o envio de notificações com base na nuvem. Ele fornece aos desenvolvedores uma capacidade altamente escalável, flexível e econômica para publicar mensagens de um aplicativo e imediatamente entregá-las aos assinantes ou outros aplicativos.

O Amazon SNS fornece uma interface simples de serviços da Web que pode ser usada para criar tópicos desejados para notificar aplicativos (ou pessoas), inscrever clientes nesses tópicos, publicar mensagens e fazer com que essas mensagens sejam fornecidas ao protocolo de escolha dos clientes (ou seja, HTTP, e-mail etc.). O Amazon SNS entrega notificações aos clientes usando um mecanismo “push” que elimina a necessidade de verificação periódica ou “poll” para novas informações e atualizações. O Amazon SNS pode ser alavancado para criar fluxos de trabalho altamente confiáveis e acionados por eventos e aplicativos de mensagens sem a necessidade da gestão complexa de middleware e aplicativos. Os usos potenciais do Amazon SNS incluem o monitoramento de aplicativos, sistemas de fluxo de trabalho, atualizações de informações relacionadas a horários, aplicativos móveis e muitos outros. Assim como ocorre com todas as Amazon Web Services, não há a necessidade de investimentos prévios e você paga somente pelos recursos que usar.

O Amazon SNS fornece mecanismos de controle de acesso para assegurar que os tópicos e as mensagens serão protegidos contra o acesso não autorizado. Os proprietários de tópicos podem definir políticas para um tópico que restrinja quem pode publicar ou assinar um tópico. Além disso, os proprietários de tópicos podem assegurar que as notificações sejam criptografadas ao especificar que o mecanismo de entrega deve ser HTTPS.

O acesso ao Amazon SNS é concedido com base em uma conta AWS ou um usuário criado com o IAM AWS. Uma vez autenticada, a conta AWS tem acesso completo a todas as operações do usuário. An AWS

IAM user however only has access to the operations and topics which they have been granted access to via policy. Por padrão, acesso para cada tópico individual é restrito para a conta AWS que o criou. No entanto, um cliente pode permitir que outros acessem uma fila, usando uma política gerada pelo SNS ou uma política escrita pelo usuário.

Segurança do Amazon CloudWatch

O Amazon CloudWatch é um serviço da Web que fornece monitoramento para recursos da nuvem da AWS, começando com o Amazon EC2. Ele fornece visibilidade sobre a utilização de recursos, desempenho operacional e padrões de demanda geral, incluindo métricas como utilização de CPU, leituras e gravações do disco e tráfego de rede.

O Amazon CloudWatch requer, como todos os serviços AWS, autenticação para cada solicitação feita à sua API de controle para que somente os usuários autenticados possam acessar e gerenciar o CloudWatch. As solicitações são assinadas com uma assinatura de HMAC-SHA1 criada a partir da solicitação e da chave privada do usuário. Além disso, a API de controle do Amazon CloudWatch só é acessível através de pontos de acesso criptografados com SSL.

Um cliente pode controlar o acesso ao Amazon CloudWatch criando usuários para a sua conta AWS usando o IAM da AWS e controlar quais operações do CloudWatch esses usuários tem permissão para chamar.

Segurança do Auto Scaling

O Auto Scaling permite que os clientes expadam ou reduzam automaticamente sua capacidade do Amazon EC2 de acordo com as condições definidas para que o número de instâncias do Amazon EC2 seja dimensionado perfeitamente durante os picos de demanda para manter o desempenho e permite a redução automática durante as baixas de demanda para minimizar os custos.

O Auto Scaling requer, como todos os serviços AWS, autenticação para cada solicitação feita à sua API de controle para que somente os usuários autenticados possam acessar e gerenciar o Auto Scaling. As solicitações são assinadas com uma assinatura de HMAC-SHA1 criada a partir da solicitação e da chave privada do usuário.

Um cliente pode controlar o acesso ao Auto Scaling criando usuários para a sua conta AWS usando o IAM da AWS e controlar quais APIs do Auto Scaling esses usuários tem permissão para chamar.

Segurança do Amazon CloudFront

O Amazon CloudFront exige que todas as solicitações feitas à sua API de controle sejam autenticadas para que somente os usuários autenticados possam criar, modificar ou excluir suas próprias distribuições do Amazon CloudFront. As solicitações são assinadas com uma assinatura de HMAC-SHA1 criada a partir da solicitação e da chave privada do usuário. Além disso, a API de controle do Amazon CloudFront só é acessível através de pontos de acesso criptografados com SSL.

Não há nenhuma garantia de durabilidade dos dados mantidos em pontos de presença do Amazon CloudFront. O serviço ao longo do tempo pode remover os objetos de locais periféricos se esses objetos não são solicitados com frequência. A durabilidade é fornecida pelo Amazon S3, que funciona como o servidor de origem para o Amazon CloudFront armazenando as cópias originais e definitivas de objetos entregues pelo Amazon CloudFront.

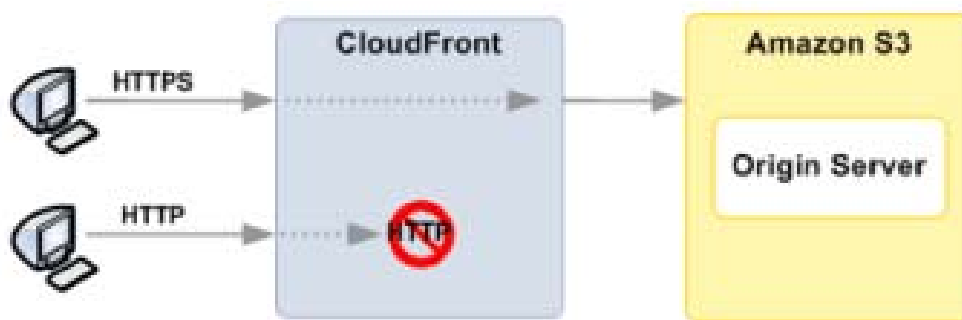
Se deseja controlar quem pode baixar o conteúdo do Amazon CloudFront, você pode habilitar o recurso de conteúdo particular do serviço. Este recurso tem dois componentes: o primeiro controla como os pontos de presença do Amazon CloudFront acessam seus objetos no Amazon S3. O segundo controla como o conteúdo é entregue desde os pontos de presença do Amazon CloudFront até usuários da internet.

Para controlar o acesso às copias originais de seus objetos no Amazon S3, o Amazon CloudFront permite criar uma ou mais "Identidades de origem de acesso" e associá-las às suas distribuições. Quando uma Identidade de acesso de origem é associada a uma distribuição do Amazon CloudFront, a distribuição usará essa identidade para recuperar objetos do Amazon S3. Você pode usar recurso ACL do Amazon S3, que limita o acesso à Identidade de acesso de origem assim que a cópia original do objeto não pode ser lida de maneira pública.

Para controlar quem pode fazer o download de seus objetos a partir dos pontos de presença do Amazon CloudFront, o serviço usa um sistema de verificação de URL assinada. Para utilizar este sistema, em primeiro lugar você cria um par de chaves pública e privada e carrega a chave pública para sua conta através do website da Amazon Web Services. Em segundo lugar, você configura a sua distribuição do Amazon CloudFront para indicar quais contas serão autorizadas a assinar as solicitações, você pode indicar até cinco contas da AWS em que confia para assinar as solicitações. Em terceiro lugar, à medida que você recebe solicitações você cria documentos de políticas que indiquem as condições sob as quais você deseja que o Amazon CloudFront ofereça o seu conteúdo. Estes documentos de políticas podem especificar o nome do objeto que é solicitado, a data e hora do pedido, o IP de origem (ou intervalo CIDR) do cliente que fez a solicitação. Então você calcula a codificação RSA-SHA1 do seu documento de políticas e assina-o usando sua chave privada. Em quarto lugar, você inclui o documento de políticas codificado e a assinatura como parâmetros de sequência de caracteres de consulta quando você faz referência aos seus objetos. Quando o Amazon CloudFront receber uma solicitação, ele irá decodificar a assinatura usando a sua chave pública. O Amazon CloudFront oferecerá apenas solicitações que possuem documentos de políticas válidos e assinatura correspondente.

Observe que o conteúdo privado é um recurso opcional que deve ser habilitado quando você configura a sua distribuição do CloudFront. O conteúdo entregue sem esse recurso habilitado será legível de forma pública por qualquer pessoa.

O Amazon Cloudfront também pode transferir o conteúdo em uma conexão criptografada (HTTPS) para autenticar o conteúdo entregue aos usuários. Por padrão, o Amazon Cloudfront aceitará solicitações através de protocolos HTTP e HTTPS.

Se você preferir, também pode configurar o Amazon Cloudfront para exigir HTTPS em todas as solicitações e não permitir as solicitações através de HTTP. Para solicitações HTTPS, o Amazon Cloudfront também vai utilizar o HTTPS para recuperar o objeto do Amazon S3 para que seja criptografado sempre que for transmitido.

Os logs do Amazon Cloudfront Access contêm um conjunto abrangente de informações sobre as solicitações de conteúdo, incluindo o objeto solicitado, a data e hora do pedido, a pontos de presença servindo a solicitação, o endereço de IP do cliente, o referrer e o agente de usuário. Para habilitar os logs de acesso apenas especifique o nome do bucket Amazon S3 para armazenar os logs quando você configurar sua distribuição do Amazon CloudFront.

Segurança do Amazon Elastic MapReduce (Amazon EMR)

O Amazon Elastic MapReduce exige que todas as solicitações feitas à sua API sejam autenticadas para que somente os usuários autenticados possam criar, modificar ou excluir seus fluxos de trabalho. As solicitações são assinadas com uma assinatura de HMAC-SHA1 criada a partir da solicitação e da chave privada do usuário. O Amazon Elastic MapReduce fornece pontos de acesso SSL para acessar as suas APIs de serviço web e o console.

Ao iniciar fluxos de trabalho em nome de um cliente, o Amazon Elastic MapReduce configura um grupo de segurança do Amazon EC2 do nó mestre para permitir somente o acesso externo via SSH. O serviço cria um grupo de segurança separado dos receptores que não permite qualquer acesso externo. Para proteger as informações dos clientes e conjuntos de dados de saída, o Amazon Elastic MapReduce transfere os dados de e para o S3 usando SSL.

APÊNDICE – GLOSSÁRIO DE TERMOS

AMI: uma Amazon Machine Image (AMI) é uma imagem de máquina criptografada armazenada no Amazon S3. Ela contém todas as informações necessárias para inicializar as instâncias de um software de cliente.

API: a Application Programming Interface (API) é uma interface em ciência da computação que define as maneiras pelas quais um programa aplicativo pode solicitar serviços de bibliotecas e/ou sistemas operacionais.

Autenticação: a autenticação é o processo de determinar se alguém ou alguma coisa é realmente quem ou o que ele declara ser.

Zona de disponibilidade: os locais do Amazon EC2 são compostos pelas regiões e pelas Zonas de disponibilidade. As Zonas de disponibilidade são as posições distintas que são projetadas para serem isoladas das falhas em outras Zonas da disponibilidade e fornecem rede de conectividade acessível e de baixa latência para outras Zonas de disponibilidade da mesma região.

Bucket: um recipiente para objetos armazenados no Amazon S3. Cada objeto está contido em um bucket. Por exemplo, se o objeto nomeado photos/puppy.jpg é armazenado no bucket johnsmith, então é abordado usando a URL http://johnsmith.s3.amazonaws.com/photos/puppy.jpg.

Bloco CIDR: endereços de IP de roteamento sem classe entre domínios.

EBS: o Amazon Elastic Block Store (EBS) fornece volumes de armazenamento em nível de bloco para uso com instâncias do Amazon EC2. Os volumes do Amazon EBS são armazenamentos fora da instância que persiste independentemente da duração de uma instância.

HMAC-SHA1: em criptografia, uma chave Hash Message Authentication Code (HMAC ou KHMAC), é um tipo de código de autenticação de mensagem (MAC) calculado utilizando um algoritmo específico que envolve uma função de hash criptográfico em combinação com uma chave secreta. Como com qualquer MAC, ele pode ser usado simultaneamente para verificar a integridade dos dados e a autenticidade de uma mensagem. Qualquer função de hash criptográfico iterativo, tais como MD5 ou SHA-1, pode ser usada no cálculo de um HMAC; o algoritmo MAC resultante é chamado de HMAC-MD5 ou HMAC-SHA1. Qualquer função de hash criptográfico iterativo, tais como MD5 ou SHA-1, pode ser usada no cálculo de um HMAC; o algoritmo MAC resultante é chamado de HMAC-MD5 ou HMAC-SHA1.

Hypervisor: um hypervisor, também chamado de Monitor de máquina virtual (VMM), é um software de virtualização de plataforma de hardware/software de computador que permite que vários sistemas operacionais executem simultaneamente em um computador host.

IAM do AWS: o Identity and Access Management da AWS (IAM da AWS) permite que o cliente crie vários usuários e gerencie permissões para cada um desses usuários a partir de sua conta da AWS.

Endereço de IP: endereço de IP (Internet Protocol) é um rótulo numérico que é atribuído aos dispositivos que participam de uma rede de computador utilizando o protocolo de Internet para a comunicação entre seus nós.

Falsificação de IP: criação de pacotes de Internet Protocol (IP) com um endereço IP de origem forjado, chamado de falsificação, com a finalidade de dissimular a identidade do remetente ou representando um outro sistema de

computação.

Objeto: entidades fundamentais armazenadas no Amazon. Os objetos consistem em metadados e dados de objeto. A porção de dados é opaca para Amazon S3. Os metadados são um conjunto de pares de nome e valor que descrevem o objeto. Estes incluem alguns metadatas padrão tais como a data da última modificação e metadata HTTP padrão como Content-Type. O desenvolvedor também pode especificar metadados personalizados no momento em que o objeto é armazenado.

Paravirtualização: em computação, paravirtualização é uma técnica de virtualização que apresenta uma interface de software para máquinas virtuais que é semelhante, mas não idêntico do hardware subjacente.

Varredura de porta: uma varredura de porta é uma série de mensagens enviadas por alguém que está tentando invadir um computador para saber quais serviços de rede de computador cada associado com um número de porta "conhecido" o computador fornece.

Serviço: Software ou computação com capacidade fornecida através de uma rede (por exemplo, EC2, S3).

Firewall estável: em computação, um firewall estável (qualquer firewall que fornece pacote de inspeção estável (SPI) ou inspeção estável) é um firewall que mantém o controle sobre o estado das conexões de rede que (tais como fluxos de TCP, comunicação UDP) trafegam através dele.

Instância virtual: uma vez que um AMI seja lançado, o sistema resultante em execução é referido como uma instância. Todas as instâncias baseadas na mesma AMI começam idênticas e qualquer informação sobre eles é perdida quando as instâncias são concluídas ou na ocorrência de falhas.

X.509: em criptografia, X. 509 é um padrão ITU-T para uma infraestrutura de chave pública (PKI) para Single Sign-On (SSO) e infraestrutura de gerenciamento de privilégio (PMI). O X. 509 especifica, entre outras coisas, formatos padrão para certificados de chave públicos, listas de certificados revogados, certificados de atributo e um algoritmo de validação de caminho de certificação.

Alterações desde a última versão: (Agosto de 2010)

- Adição do AWS Identity and Access Management (AWS IAM)
- Adição da segurança do Amazon Simple Notification Service (SNS)
- Adição da segurança do Amazon CloudWatch
- Adição da segurança do Auto Scaling
- Atualização do Amazon Virtual Private Cloud (Amazon VPC)
- Atualização do ambiente de controle
- Remoção de gerenciamento de riscos como foi descrito em detalhes em um whitepaper separado

Alterações desde a última versão (Novembro de 2009):

- Revisões importantes

Alterações desde a última versão (Julho de 2009):

- Alteração da seção de Certificações e acreditações para refletir a SAS 70
- Adição do Amazon Virtual Private Cloud (Amazon VPC)
- Adição de seção de credenciais de segurança para realçar a autenticação Multi-gateway de internet AWS e rotação de chaves
- Adição da segurança do Amazon Relational Database Service (Amazon RDS)

Alterações desde a última versão (Setembro de 2008):

- Adição dos princípios de design seguro
- Atualização de informações de segurança física e inclusão de verificação de antecedentes
- Seção Backup atualizada para maior clareza com relação ao Amazon EBS
- Atualização da seção de segurança do Amazon EC2 para incluir:
- SSHv2 baseado em certificação
- Diagrama e detalhes do grupo de segurança em vários níveis
- Descrição do hypervisor e do diagrama de isolamento de instância
- Separação de falhas
- Adição do gerenciamento de configuração
- Seção do Amazon S3 atualizada para detalhes e clareza
- Adição da desativação do dispositivo de armazenamento
- Adição de segurança do Amazon SQS
- Adição de segurança do Amazon CloudFront
- Adição de segurança do Amazon Elastic MapReduce

Avisos